

Serial No. 09/911,061
Group Art Unit 2151
2001-0056 Brief on Appeal



IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

In re Application of:

Y. Chen, et al.

Case: 2001-0056

Serial No.: 09/911,061

Art Unit: 2151

Examiner: Nghi V. Tran

Filed: 07-23-01

Title: Flexible Automated Connection to Virtual Private Networks

COMMISIONER FOR PATENTS

P.O. BOX 1450

Alexandria, VA 22313-1450

SIR:

BRIEF ON APPEAL

Appellants submit the present brief pursuant to a Notice of Appeal, mailed April 11, 2007, from a decision of the Examiner, dated October 11, 2006, finally rejecting claims 22-27 - all of the claims remaining in the present application.

(i). Real Party in Interest

AT&T Corp. is the real party in interest by virtue of an assignment of Yihsiu Chen, Mark Jeffrey Foladare, Shelley B. Goldman, Thomas Joseph Killian, Norman Loren Schryer, Kevin Stone, and Roy Phillip Weber recorded July 23, 2001 at Reel/Frame 012048/0899.

(ii). Related Appeals and Interferences

This is the first appeal in the above-identified application.

(iii). Status of the Claims

The application contains claims 22-27, all of which stand finally rejected under 35 U.S.C. §103(a). The Appendix contains a complete copy of the claims now pending in the application. Appellants appeal the rejection of claims 22-27.

(iv). Status of the Amendments

No amendment was filed subsequent to final rejection. However, the final rejection from which the present appeal was taken was a substantial duplicate of the prior non-final rejection, to which a full response was filed.

(v). Summary of Claimed Subject Matter

Generally, login by a LAN client (FIG. 3, 304, ..., 310) with a illustratively portable (p.23, line 26 through p.24, line 5) network interface unit (NIU, 302 in FIG. 3, and all of FIG. 4), permits device and network addressing, authentication, and other configuration operations to be achieved using a web page-based GUI (FIGs. 7-16) for establishing VPN tunnels from LAN clients to desired VPN destinations (FIG. 3, 398 and 399). Illustrative NIUs (302) include a DHCP server (FIG. 4, 457) and provide encryption-decryption (FIG. 4, 460) and encapsulation-decapsulation of data packets (FIG. 4, 440 and 460) for communication with illustrative VPN nodes 398 and 399 in FIG.3 through firewall (395) and using the services of security portal (390). Configuration and connection of clients are further enhanced by a built-in DNS server

(FIG. 4, 435) and other functional servers to provide a high degree of autonomy in establishing connections to a desired VPN gateway via an ISP or other public and/or private network links to. The interface unit then performs required authentication exchanges, and required encryption key exchanges. More specifically for the method of independent claim 22:

22. A method practiced at a network interface unit (NIU) directly connected to at least one local area network (LAN), said NIU also being connected to a non-secure node of a second network, which second network is in packet communication with at least one access node of a secure virtual private network (VPN), the method comprising	FIG. 3, (302); and p. 6, line 27 through p. 7, line 2 show and describe a network interface unit (NIU) 302 directly connected to a LAN (301) (among other LAN clients); NIU 302 is also shown in FIG. 3 and described at p. 11, lines 5-10 to be connected via illustrative wireless modem (303), and cable ISP (323), among other links, to the insecure Internet (350) for establishing secure links to a VPN gateway (FIG. 3, (390) and (395); p. 7, lines 9-16); FIG. 2 and the description at p. 10, line 28 through p. 11, line 18 describe the relationship between FIGs. 2 and 3;
receiving data packets from at least one device on said at least one LAN,	packets from at least one of the devices (304, 305, 306, 307 ..., 310) on LAN (301) are received at NIU (302); see FIG. 4 and p. 12, lines 6-13
multiplexing said data packets into at least one packet data stream,	NIU (302), shown generally in FIG. 4, multiplexes received packets into at least one packet data stream in input unit 410 of FIG. 4 as described at p. 12, lines 6-13;
modifying said at least one packet data	modifying said at least one packet data

stream in a security server in said NIU in accordance with a secure communications protocol by encrypting packets in said at least one packet data stream and encapsulating resulting encrypted packets, and	stream in said NIU (302) by encrypting said at least one packet data stream in IPSEC SERVER (470) shown in FIG. 4 and described at p. 14, line 28 through p. 15, line 16, and encapsulating resulting encrypted packets in cooperation with controller (440) shown in FIG. 4 and described at p. 14, line 28 through p. 15, line 16;
providing network destination address information from a Domain Name System (DNS) server for at least selected ones of said at least one packet data stream .	DNS Server (435) in FIG. 4 provides destination address information, as described at p. 16, lines 22-25 and p. 17, lines 23-25 (with reference to FIG. 4). The operation of DNS Server (435) is further illustrated in FIG. 6 and described (with other NIU configuration elements) at p.23, lines 3-15.

For purposes of this appeal, claims 22-27 rise or fall together.

(vi). Grounds for Rejection to be Reviewed on Appeal

The issue is whether claims 22-27 (all of the claims) were properly rejected as obvious under 35 U.S.C. §103(a) over Liu in light of Larson. Accordingly, an underlying issue is whether the final rejection of claims 22-27 are in compliance with the law of obviousness as announced by the Supreme Court in *KSR International Co. v. Teleflex Inc* 550 U.S. ___, 82 USPQ2d 1385 (2007) and the *Patent and Trademark Office Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in view of the Supreme Court Decision in KSR International Co. v. Teleflex Inc* published in the Federal Register, vol. 72, No. 195, pp57526-57535 on October 10, 2007. The cited USPTO document will be referred to herein simply as “Guidelines,” and the Supreme Court decision as “KSR.”

(vii). Arguments

Appellants assert that Examiner has failed to make the necessary factual inquiries and *correct and complete* factual findings necessary to provide the underpinnings required to establish obviousness of claims 22-27 in accordance with *KSR* (and other applicable Supreme Court decisions cited in *KSR*) and the *Guidelines*. In this regard, Examiner has not ensured that the written record includes *correct and complete* findings of fact concerning the state of the art and the teachings of the references applied. In addition Examiner has not articulated the level of ordinary skill in the pertinent art that would give rise to combining differently directed individually self-sufficient references. Further, Examiner has not complied with the requirements of 35 U.S.C. 132 to provide sufficient notice of the reasons for the rejection of claims 22-27 so that appellants can decide how to proceed.

A. Legal Standards

35 U.S.C. 103(a) states:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

In *KSR International Co. v. Teleflex Inc.* 550 U.S. ___, 82 USPQ2d 1385 (2007) (“*KSR*”) the U.S. Supreme Court rejected certain techniques for ascertaining obviousness in favor of reaffirming its prior decision in *Graham v. John Deere Co.* 383 U.S. 1, 148 USPQ 459 (1966) – hereinafter “*Graham*.” The USPTO *Guidelines* are intended to assist USPTO personnel to make a proper determination of obviousness under 35 U.S.C. 103 in view of *KSR* and provide an appropriate supporting rationale. (*Guidelines*, p. 57526)

Graham has noted that obviousness is a question of law based on underlying factual inquiries:

- (1) Determining the scope and content of the prior art;

- (2) Ascertaining the differences between the claimed invention and the prior art; and
- (3) Resolving the level of ordinary skill in the pertinent art.
(*Guidelines*, p. 57527)

B. Discussion of the Prior Art

1. U.S. Patent 6,079,020 to Liu (hereinafter “Liu”)

Liu relates to techniques for managing secure virtual private networks (VPNs) over public or otherwise insecure data communication infrastructures. (Liu, col. 1, lines 9-12) Managing a large number of VPN gateways, which are geographically distributed throughout a public network, can be a time-consuming and error-prone task. Each time a VPN is modified VPN gateways must be reconfigured to reflect the modifications. (Liu, col. 2, lines 30-35) This process is time-consuming because each VPN gateway must presently be reconfigured with network address information specifying which communications are to be transmitted securely, and which ones are not. (Liu, col. 2, lines 38-41) A VPN administrator must presently enter this configuration information manually, which can be a time consuming task. Furthermore, it is very easy to make mistakes in translating a policy into network address specifications and in entering the long strings of number that make up network address specifications. (Liu, col. 2, lines 52-58)

Liu’s solution to overcome these limitations includes a system that operates by receiving a command specifying an operation on the virtual private network. The system determines which virtual private network gateways are affected by the command. The system then automatically translates the command into configuration parameters for virtual private network gateways affected by the command. These configuration parameters specify how the virtual private network gateways handle communications between specific groups of addresses on the public data network. The system then transmits the configuration parameters to the virtual private network gateways affected by the command, so that the virtual private network gateways are configured to implement the command. (Liu, col. 3, lines 9-21)

These configuration parameters are received at the VPN gateway. The system uses these configuration parameters to determine whether the source and destination

addresses of a communication between nodes in the public data network belong to the same virtual private network. If the source and destination addresses belong to the same virtual private network, the system ensures that the communication is transmitted securely over the public data network. (Liu, col. 3, lines 22-31)

Liu's FIG. 1 illustrates a public network 100 including VPN gateways 115, 125, 135, 145, and 155 operating under control of a VPN management station 160. (Liu, col. 3, lines 64-67) Liu provides a number of different VPN management commands, including commands to create a VPN, to modify a VPN and to delete a VPN. (Liu, col. 3, lines 32-38)

2. U.S. Patent Publication 2004/0107286 A1 by Larson, *et al.*, (hereinafter "Larson") seeks to improve secure communication using VPNs. Overall, Larson is directed to improvements in securely communicating between two network locations using VPNs. Larson describes a secure mechanism for communicating over the Internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a two-layer encryption format, special TARP terminals and special TARP routers. (Larson, [009]) In particular, Larson asserts

The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is *built on top of the existing Internet protocol (IP)*. (Larson, [0024]) [Emphasis Added.]

The TARP protocol relies on so-called hopping techniques, in accordance with which "[e]ach pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving)" (Larson, [0023]) Larson also teaches means for distinguishing between TARP packets and other cryptographically valid packets, such as IPsec packets. Larsen's TARP protocol is not used to handle IPsec patents. (Larson, [0285])

Overall, VPN connectivity using Larson's TARP protocol does not allow end-to-end delivery of packets in the normal manner (*e.g.*, that employed by Liu). Instead,

Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. (Larson [0010])

Further, using the hopping techniques described in Larson at [0023] and elsewhere, Larson employs hop blocks of allowed and expected pairs of continually changing IP addresses to be prepared to check arriving packets under TARP protocol. (Larson, [0132])

Another feature introduced in Larson (and cited in Examiner's Final Rejection) is the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function. (Larson, [261]) This feature of Larson builds on the TARP protocol introduced in Larson, including use of the associated "hopping" techniques and TARP packet discrimination that are built on top of the normal IP protocol. (Larson, FIG. 26 and [267] and [268])

C. The Examiner's Rejection

The October 11, 2006 Final Office action, from which the present appeal is taken, substantially repeated the grounds cited in the February 7, 2006 Office action for rejections under 35 U.S.C. §103(a). The Liu and Larson references were applied in the same manner as in the previous Office action. In particular, Examiner concluded that Liu described all of the steps of present claim 22 except for the step of "providing network destination address information from a Domain Name System (DNS) server for at least selected ones of said at least one packet stream," but that that step was taught by Larson. It was therefore concluded that claim 22 was obvious over Liu in light of Larson.

D. Appellants' Response to Examiner's
Final Rejection of Claims 22-27

1. Summary of Appellants' Response

a. *Weight Accorded Claim Preamble* Examiner has failed to afford patentable weight to applicants' preamble in claim 22, saying it "merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or

structural limitations are able to stand alone.” In the context of the rejection of claim 22 that finding is manifestly incorrect.

b. *Examiner Did Accord Weight to Preamble – And Got it Wrong*

Contrary to Examiner’s assertion regarding the preamble, the final rejection expressly recites that “Liu teaches a method practiced at a network interface unit (NIU) directly connected to at least one local area network (LAN)” (Final Rejection, paragraph 4) This application of Liu to the preamble is factually in error. Moreover, Examiner’s dismissal of appellants’ arguments in response to the rejection of claim 22 in the prior non-final rejection regarding the preamble prejudiced applicants by avoiding the creation of a written record of important reasons for rejecting the claim under 35 U.S.C. § 103(A).

c. *Liu is Directed to a Different Purpose Not Employing Applicants’ Steps*

Liu describes methods and systems for automatically translating a command into parameters for configuring virtual private network gateways at known locations in a VPN that are affected by the command. Liu does not teach or suggest a “NIU directly connected to at least one ... LAN,” thereby permitting portability and use at many different LAN locations.

d. *One Skilled in the Relevant art would have no reason for “providing network destination address information from a Domain Name System (DNS) server...” in Liu, and no reason to incorporate Larson’s teachings in Liu*

Because Liu stores all needed address information at respective VPN gateway nodes, no resort to a DNS server is required or useful in Liu. Combining Larson, a reference that describes VPNs and DNS functionality (though with many unique differences from standard IP VPNs), with Liu’s teachings that do not use or require DNS functionality is purely gratuitous. No showing of why a person of ordinary skill would find it obvious to incorporate Larson’s teachings in Liu has been presented in the Final Rejection.

2. Detailed Response to the Final Rejection

a. *Weight Accorded Claim Preamble*

In the final rejection Examiner concluded that patentable weight should not be accorded applicants' preamble in claim 22, saying it "merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone." In the context of claim 22 that finding is manifestly incorrect.

First, the preamble recites where in an overall network context the present invention is practiced: at a network interface unit (NIU). Second, the NIU is said to be "directly connected to at least one local area network (LAN). Third, the NIU is further characterized as "also being connected to a non-secure node of a second network, which second network is in packet communication with at least one access node of a secure virtual private network (VPN)...." Thus, the preamble provides essential linking functionality with other steps of the method of claim 22.

In addition to providing operative relationships between the NIU and other network elements, other steps of claim 22 depend on the preamble for completeness. Thus, the "receiving" step refers to "receiving data packets from at least one device on said at least one LAN." Only the preamble provides the antecedent and operative relationship with this NIU step. Similarly, in the "modifying" step, the security server is said to be "in said NIU."

b. *Examiner Did Accord Weight to Preamble – And Got it Wrong*

Contrary to Examiner's statement (in paragraph 19 of the Final Rejection), the preamble was accorded weight in rejecting claim 22. (See paragraph 4 of the Final Rejection) Initially, it is respectfully submitted that Examiner's characterization of Liu generally is in error and the reading of Liu's FIGs. 1 and 2 and Abstract on claim 22 is a misapplication of the purpose and teachings of Liu.

For example, in Liu's FIG. 2 cited by Examiner is a flow chart illustrating the processing of a packet being transmitted from one member of a VPN to another member of the VPN over a public data network. Step 210 in FIG. 2 of Liu describes "RECEIVE OUTBOUND DATA PACKET AT VPN GATEWAY" (gateways 115, 125, 135, 145 and 155 in Liu's FIG. 1). Examiner applied step 210 in FIG. 2 to appellants' step of "receiving data packets from at least one device on said LAN." Since appellants'

“receiving” step is performed at their NIU (per preamble to appellants’ claim 22). So, Examiner was identifying appellants’ NIU with one of Liu’s VPN gateways.

But Liu’s VPN gateways, unlike applicants’ NIU, are not “directly connected to at least one local area network (LAN). Instead, each of Liu’s VPN gateways are connected to a respective LAN through a respective router (114, 124, or 134 in Liu’s FIG. 1). In another embodiment of the present invention, the VPN gateways handle communications between remote clients coupled to the public data network through an internet service provider (ISP). Thus in all cases, Liu has no method that is practiced at an element that is “directly connected to at least one local area network (LAN).”

c. *Liu is Directed to a Different Purpose Not Employing Applicants’ Steps*

From Liu’s FIGs. 1 and 2 and Abstract, it is clear that Liu is concerned with the automatic configuration of an entire virtual private network including a plurality of virtual private network (VPN) gateways. Liu requires the receipt of a command to specify the operation of the network and then determines which VPN gateways are necessarily involved. The command is accordingly translated into configuration parameters specifying how the VPN gateways should handle communications between specific groups of addresses on the public data network. The configuration parameters are then sent to the VPN gateways affected by the command.

In particular, Liu’s teachings provide that a command specifying a network operation received at VPN management station 160 for translation into configuration information for delivery to VPN gateways affected by the command. (Liu, col 3, lines 8-14.) *VPN groups* are established in the Liu system and VPN processing is performed and packets delivered when it is determined that source and destinations are members of the same VPN group. (Liu, FIG. 2, 220,240 and 250.)

Configuration Parameters, as defined in Liu at col. 4, lines 48-50, are “parameters sent to a VPN gateway to configure the VPN gateway to appropriately handle communications between members of VPNs.” Importantly, configuration parameters delivered to gateways include specific groups of addresses between which communications are to be transmitted securely. In a variation on this embodiment, the configuration parameters include Internet Protocol (IP) addresses. Thus, address

information is provided to gateways to *define VPN groups* and to *individual IP addresses*. (Liu, col. 3, lines 39-43.) Further illustration of the management of network addresses and the express provision of them to particular gateways is provided by FIGs. 8-10 and the discussion thereof at col. 10, line 7 through col. 11, line 9.

Appellants' claim 22, on the other hand is connected directly to a LAN to allow connection of devices on the LAN to connect through a VPN over a non-secure network.

d. *One Skilled in the Relevant art would have no reason for "providing network destination address information from a Domain Name System (DNS) server..." in Liu, and no reason to incorporate Larson's teachings in Liu*

Examiner's rejection based on a DNS server function provided by Larson imports a function not used or needed in Liu. In respect of its configuring functionality, Liu communicates from a central management station 160 to the several VPN gateways, each at known locations. Thus, no "providing network destination address information from a Domain Name System (DNS) server" is needed, nor would any such DNS server be of use for such configuration operations.

In respect of destination-to-destination communications of the type described with reference to Liu's FIGs. 1 and 2, Liu requires that the destination address be provided at the source. See, for example, Liu at col. 7, lines 8-67 cited by Examiner. (Note: the reference in Liu at line 20 to FIG. 3 is believed to be in error. The cited step numbers associated with the intended FIG. are those for FIG. 2.) Importantly, Liu describes the functioning at step 220 to be directed to "whether or not the source and destination addresses for the data packet are both members of the same VPN group." Thus the destination address is already present in the packets that arrive at the VPN gateways of Liu; no need for a DNS lookup exists.

Examiner cites to Larson as providing DNS functionality, but not to the need (or appropriateness) in Liu to use such DNS functionality. For those packets that are not addressed to members of the same VPN group, packet discard or unencrypted transmission on the Internet are alternatives recognized by Liu. See, Liu, col. 7, lines 35-40. If a destination address is not one that is in the same VPN group as the origination address, it can still be delivered or discarded. Employing DNS when the destination

address is already known (as in Liu) makes no common sense. Moreover, both the existing point-to-point communication of Liu and the centralized updating of VPN gateway controls would have to be discarded or made the subject of extensive modifications if domain name addressing were to be used – none of which appear except in the imagination of the Examiner. No indication of these needed extensive changes are part of a determination of the content of the references and the state of knowledge of one of ordinary skill in the art. Examiner has provided no such factual bases.

Larson establishes secure communication using VPN techniques. But, if Liu wanted to include a particular destination in a VPN (assuming it is otherwise desirable) it would be a simple matter to add that destination to a group recognized as being included in the same group as the source. Examiner has sought to force-fit Larson as part of a combination with Liu to supply unnecessary VPN functionality because Larson chooses to use DNS functionality for some cases of interest to Larson. Appellants' claim 22 specifically states that the DNS server is used to "provide network destination address information." As noted above, Liu already has all of the destination address information that is needed.

Examiner's cite to Larson [0261] is inapposite. That paragraph states:

A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

Liu has no need to perform such a look-up function. Indeed, Liu neither uses nor has been shown to require any such domain-name functionality. Liu uses known addresses of its VPN gateways to deliver (by way of respective routers) packets containing destination addresses; these are then compared at the VPN gateways. Importantly, if DNS functionality were to be included in Liu's VPN gateways (identified in the rejection with applicants NIU), it would defeat the goal of Liu to provide a central control at the VPN management station 160 that forms a core of Liu's approach. So, not only does Liu not show or suggest "providing network destination address information from a Domain Name System server for at least selected ones of said data streams" at his VPN gateways, use of such DNS functionality at VPN gateways would be counter to Liu's approach of providing VPN gateway information from a central source.

In contradistinction, the invention defined in applicants' present claim 22, recites NIU functions including "providing network destination address information from a Domain Name System server for at least selected ones of said data streams." This is inconsistent with Liu's use of explicit IP addresses and VPN groups defined by addresses delivered as configuration parameters by Liu's centralized VPN management station 160.

The providing of destination address information in the manner recited in applicants' claim 22 confers advantages to applicants' embodiments in the form of increased flexibility and mobility. That is, reliance on Liu's rigid address format, updating from a central VPN management station 160 and rigid adherence to *VPN groups* need not be observed in applicants' claimed invention. This is especially important in applications of the present inventive methods where a user is required to move from one location to another as discussed, for example, in the specification at page 23, line 28 through page 24, line 5 where it is noted that required configuration information can readily be applied by a portable NIU.

Because it would serve no useful function and would defeat the goal of central configuration of VPNs using a VPN management station, Liu provides no suggestion of "providing network destination address information from a Domain Name System server for at least selected ones of said data streams" at a NIU. Therefore, one skilled in the art would not look to sources such as Larson to modify the teachings of Liu to include such DNS functionality at an NIU. Moreover, the DNS functionality shown in the cited portions of Larson is not performed at a NIU. Moreover, it appears from Larson's [0260-0280] and associated FIG. 26 that Larson's approach employs a DNS server 2609 and DNS proxy server 2610 communicating through a gatekeeper 2603, none of which practice applicants' method of claim 22. None of these elements in Larson practice the claimed method steps at a NIU.

No suggestion has been identified by Examiner that Larson performs his DNS functioning at a NIU or that Larson (or Liu) contemplate use of a NIU having the functionality described in claim 22. There is simply no basis for importing a technique from a non-existent NIU in Larson into a non-existent NIU in Liu that would, in any event, defeat the purposes sought to be achieved in Liu.

d.

Examiner acknowledges that Liu does not explicitly show “providing network destination address information from a DNS server....” However, Examiner finds this “providing” step in “a method for establishing secure communication” in Larson’s paragraphs [0024], [0225], [0260-0268]. From these teachings of Larson, and further in view of Larson’s Abstract, Examiner concludes that it would have been obvious to a person of ordinary skill in the art to modify Liu by including the step of “providing network destination address information from a DNS server....” Specifically, it is said by Examiner that “one of ordinary skill in the art at the time of the invention would have been motivated in order to automatically create of [*sic.*] a VPN in response to a DNS server look-up function, citing more particularly to Larson’s [261].

Examiner’s rejection based on a DNS server function provided by Larson imports a function not used or needed in Liu. In respect of its configuring functionality, Liu communicates from a central management station 160 to the several VPN gateways, each at known locations. Thus, no “providing network destination address information from a Domain Name System (DNS) server” is needed, nor would any such DNS server be of use for such configuration operations.

In respect of destination-to-destination communications of the type described with reference to Liu’s FIGs. 1 and 2, Liu requires that the destination address be provided at the source. See, for example, Liu at col. 7, lines 8-67 cited by Examiner. (Note: the reference in Liu at line 20 to FIG. 3 is believed to be in error. The cited step numbers associated with the intended FIG. are those for FIG. 2.) Importantly, Liu describes the functioning at step 220 to be directed to “whether or not the source and destination addresses for the data packet are both members of the same VPN group.” Thus the destination address is already present in the packets that arrive at the VPN gateways of Liu; no need for a DNS lookup exists.

Examiner cites to Larson as providing DNS functionality, but not to the need (or appropriateness) in Liu to use such DNS functionality. For those packets that are not addressed to members of the same VPN group, packet discard or unencrypted transmission on the Internet are alternatives recognized by Liu. See, Liu, col. 7, lines 35-40. If a destination address is not one that is in the same VPN group as the origination address, it can still be delivered or discarded. Employing DNS when the destination

address is already known makes no common sense. Moreover, both the existing point-to-point communication of Liu and the centralized updating of VPN gateway controls would have to be discarded or made the subject of extensive modifications if domain name addressing were to be used – none of which appear except in the imagination of the Examiner.

Larson establishes secure communication using VPN techniques. But, if Liu wanted to include a particular destination in a VPN (assuming it is otherwise desirable) it would be a simple matter to add that destination to a group recognized as being included in the same group as the source. Examiner has sought to force-fit Larson as part of a combination with Liu to supply unnecessary VPN functionality because Larson chooses to use DNS functionality for some cases of interest to Larson. Appellants' claim 22 specifically states that the DNS server is used to "provide network destination address information." As noted above, Liu already has all of the destination address information that is needed.

Examiner's cite to Larson [0261] is inapposite. That paragraph states:

A second improvement concerns the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.

Larson describes a secure mechanism for communicating over the Internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a two-layer encryption format, special TARP terminals and special TARP routers. (Larson, [009]) In particular, Larson asserts

The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is *built on top of the existing Internet protocol (IP)*. (Larson, [0024]) [Emphasis Added.]

The TARP protocol relies on so-called hopping techniques, in accordance with which "[e]ach pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving)" (Larson, [0023]) Larson also teaches means for distinguishing between TARP packets and other cryptographically valid packets, such as IPsec packets. Larsen's TARP protocol is not used to handle IPsec patents. (Larson, [0285])

Overall, VPN connectivity using Larson's TARP protocol will not allow end-to-end delivery of packets in the normal manner (*e.g.*, that employed by Liu). Instead,

Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. (Larson [0010])

Further, using the hopping techniques described in Larson at [0023] and elsewhere, Larson employs hop blocks of allowed and expected pairs of continually changing IP addresses to be prepared to check arriving packets under TARP protocol. (Larson, [0132])

Another feature introduced in Larson (and cited in Examiner's Final Rejection) is the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function. (Larson, [261]) This feature of Larson builds on the TARP protocol introduced in Larson, including use of the associated "hopping" techniques and TARP packet discrimination that are built on top of the normal IP protocol. (Larson, FIG. 26 and [267] and [268])

Other changes required in Liu's teachings to incorporate Larson's DNS contribution include:

1. use of a non-standard top-level domain name...." (Larson, [0027], [0028]);
2. a modified DNS server (DNS proxy server) that transparently creates a virtual private network in response to a domain name inquiry (Larson [267]). This is in addition to a conventional DNS server (Larson, FIGs. 26 and 27 and [0268];
3. A gatekeeper server interposed between the modified DNS server and a secure target site. (Larson [0268]);
4. identification of "a special type of user" for which secure communication services are defined, so that a specialized DNS server can trap DNS requests from such special type of user. (Larson, [267])

So, not only are the Larson DNS functions unnecessary and incompatible with the Liu teachings, but incorporation of Larson's DNS teachings would require drastic changes to the Liu arrangements and operations.

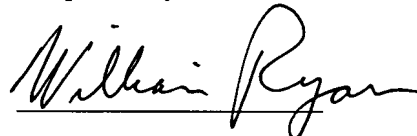
Accordingly, it is submitted that neither Liu nor Larson, nor any combination of them teach or suggest the invention of claim 22. Claims 23-27 include all of the limitations of claim 22 and are patentable over Liu or Larson, or any combination of them, for the same reasons as claim 22. Neither of Liu or Larson teaches or suggests a NIU having the functionality of the elements claimed in claims 22-27.

Conclusion

For the foregoing reasons, it is respectfully submitted that claims 22-27 as previously amended, overcome or avoid all bases for rejection and are allowable. It is requested that all claims be found allowable and passed to issue.

October 11, 2007

Respectfully submitted



William Ryan, Reg. No. 24,434

Attorney for Appellants

William Ryan, Patent Attorney

1577-D New Garden Road, Suite 300

Greensboro, NC 27410

336-286-5712

APPENDIX
(Claims on Appeal)

22. A method practiced at a network interface unit (NIU) directly connected to at least one local area network (LAN), said NIU also being connected to a non-secure node of a second network, which second network is in packet communication with at least one access node of a secure virtual private network (VPN), the method comprising
receiving data packets from at least one device on said at least one LAN,
multiplexing said data packets into at least one packet data stream,
modifying said at least one packet data stream in a security server in said NIU in accordance with a secure communications protocol by encrypting packets in said at least one packet data stream and encapsulating resulting encrypted packets, and
providing network destination address information from a Domain Name System (DNS) server for at least selected ones of said at least one packet data stream .

23. The method of claim 22 wherein said modifying said at least one packet data stream in a security server comprises modifying said at least one packet data stream in an Internet Protocol security (IPsec) server.

24. The method of claim 23 further comprising
receiving at least one stream of data packets from said non-secure network,
filtering out packets in said at least one stream of received data packets that are not from said VPN network, said filtering being performed by a firewall in said security server, said filtering producing at least one filtered stream of received data packets,
modifying said packets in said at least one filtered stream of received data packets by decrypting said packets in said at least one filtered stream of received data packets and decapsulating resulting decrypted packets to produce decapsulated decrypted packets, said decrypting and decapsulating being performed by said security server,
demultiplexing at least one stream of decapsulated decrypted received data packets to form at least one demultiplexed stream of said received data packets for delivery to said at least one LAN.

25. The method of claim 24 further comprising
authenticating client devices on said at least one LAN, and

wherein packets from authenticated client devices on said at least one LAN that are received at said network interface device are processed as packets received from said VPN.

26. The method of claim 22 wherein said non-secure node of a second network is part of said NIU.

27. The method of claim 26 wherein said at least selected ones of said at least one packet data stream are applied to said non-secure node of said second network.